# Table of Contents

# X509UserPlugin

X509 Authentication support

This plugin supports the authentication of users using X.509 certificates.

## Overview

This plugin relies on the X509UserMapping, X509Login and X509PasswdUser modules, which are included in the kit.

As a whole, this allows TWiki contributors to be automagically identified by X.509 certificate (long a wish listed in, for example: The TWiki User Authentication topic .

This plugin is used in the administration of a TWiki, and is not particularly useful for other contributors.

There are a number of configurable policy options, discussed below. However, I'm sure I didn't anticipate everyone's requrements - I stopped a while after I met mine.

The plugin proper allows you access to fields in the user certificate. This is used on the TWikiRegistration topic (Yours should, of course be in TWikiRegistration), where it allows you to specify most of the form fields from the certificate.

The %X509 variable can not be used on other pages unless you have CHANGE access to the Registration topic because a malicious user could mis-use it to expose arbitrary TWiki server state.

## Syntax Rules

There are several syntaxes for the %X509% variable. First, the syntax of an X.509 Distinguished Name (DN):

An X.509 certificate's distingushed name looks like:

```
/C=US/ST=NewYork/L=Albany/O=Megalith Corporation/OU=Executives/OU=Wayward/CN=Myway, Lost II/email
```

A typical X.509 certificate has 2 Distinguished Names: that of the certificate's *issuer* and that of the *subject*. The issuer is the authority that asserts that the certificate content is valid. The subject is the person (or in some cases, thing) that is being identified. As used here, the subject is the TWiki user. Thus, the subject's DN is of primary interest for authentication.

The subject's DN is placed in the `SSL_CLIENT_S_DN` environment variable by the webserver. It's also placed in the `REMOTE_USER` variable under `FakeBasicAuth`, which is the environment expected by this plugin.

Each /XX= is called an *element.* An element can occur multiple times; in the example, **Executives** and **Wayard** are both occurances of the **OU** element. TWiki's X509 subsystem names the first occurance **OU** and the second **OU.2**. The next would be **OU.3** and so on.

With OpenSSL, you can extract the DN from a certificate in PEM format using :

```
openssl x509 -noout -subject -inform pem (or der) -in filename
```

The %X509 variable returns certificate-related information, primarily from the client certificate.

## Common parameters

The following optional parameters are used by more than one form of the %X509% variable.

#### remove="regexp"

The value returned by the %X509% variable is modified by applying regexp as the left side of a **s///** operator. This usually specifies what string is to be removed from the value, although the full power of **s///** is available.

#### replace="string"

When the remove parameter is specified, replace specifies the replacement string. You can specify backreferences to make the substitution as powerful as you like.

#### from="issuer"

To extract data from the Issuer fields of a certificate, specify from=issuer. The default is from="user'.

#### login="DN"

The %X509% variable normally obtains its data from the `SSL_CLIENT_S_DN` environment variable. To use another DN, specify login="DN" (in the /xx=... format). Note that this overrides from="issuer" if both are specified.

## %X509{element="ele" remove="regexp" replace="string" login="DN" from="issuer"}%

Extracts element from the certificate. Typical elements are **CN**, **O**, **OU**.

## %X509{getloginname="1" remove="regexp" replace="string" login="DN" from="issuer"}%

Returns the login name (the full DN).

## %X509{getcert="component" remove="regexp" replace="string" from="issuer"}%

Extracts component from the certificate, contained in the **SSL_CLIENT_S_component** environment variable. This provides access to country codes (C /C=), Localities (L /L=), etc.

## %X509{getwikiname="1" remove="regexp" replace="string" login="DN" from="issuer"}%

Computes the (probable) wikiname that would be assigned to the specified certificate at registration.

A different wikiname may be assigned - in particular, the one offered could be claimed by somone else who registers between the expansion of this variable and the registration agent's action.

# Examples

- `%X509{getcert="Email"}%` rich@megalith.example.com
- `%X509{"CN"}%` Myway, Lost II
- `%X509{"CN" remove="^.*, "}%` Myway
- `%X509{"CN" remove="^(.*), (.*$)" replace="$2$1"}%` LostIIMyway
- `%X509{"emailAddress" from="issuer" remove="(?:\@(.*))$" replace=" at $1.NOSPAM" }%` certificates at security.megalith.example.com.NOSPAM
- `%X509{"CN" from="issuer"}%` Megalith Certificate Authority

# Plugin Settings

All settings for this plugin are stored in the configure database, and are managed by the system administrator. They are described below.

# Plugin Installation Instructions

***Note:*** You do not need to install anything on the browser to use this plugin. The following instructions are for the administrator who installs the plugin on the TWiki server.

- Download the ZIP file from the Plugin Home (see below)
- Unzip **X509UserPlugin.zip** in your twiki installation directory. Content:

| File: | Description: |
|---|---|
| **data/TWiki/X509UserPlugin.txt** | Plugin topic |
| **data/Sandbox/TWikiRegistration.txt** | Sample registration topic |
| **lib/TWiki/Plugins/X509UserPlugin.pm** | Perl module |
| **lib/TWiki/Plugins/X509UserPlugin/Config.spec** | Configure specification |
| **lib/TWiki/Configure/Checkers/Plugins/X509UserPlugin/System.pm** | Configuration checker |
| **lib/Twiki/LoginManager/X509Login.pm** | Perl module |
| **lib/TWiki/Users/X509PasswdUser.pm** | Perl module |
| **lib/TWiki/Users/X509UserMapping.pm** | Perl module |
| **lib/TWiki/Users/X509UserMapping/Cert.pm** | Perl module |

- Prepare your environment
  - If you have previously been using Apache login, edit your .htpasswd file to include WikiName before the email field.
  - Modify your webserver's configuration to support SSL and FakeBasicAuth - see below for an example.
- Configure the Plugin:
  - TWiki 4.0 and up: Run the configure script to enable the Plugin
  - Change the Plugin settings as needed
  - Update your Registration topic
- Test if the installation was successful:
  - Register and login

## Configure settings

Here are the configure settings for this facility.

### {Plugins}{X509UserPlugin}{Debug}

Enables debugging - currently mostly log messages from the plugin. May be useful to determine why things aren't working as you expect.

### {Plugins}{X509UserPlugin}{ForceAuthentication}

Because X.509 Certificates are automatically presented by the browser (assuming your webserver is properly setup), it is convenient to automagically login every user. Enable this option to cause authentication requests for all views except your registration page.

To force authentication for other scripts, add them to the {AuthScripts} configuration variable

### {Plugins}{X509UserPlugin}{RegistrationTopic}

The topic name (Don't include the webname, which is either the main or the twiki web) of the user registration topic - normally TWikiRegistration. Only this topic (or users with CHANGE access to it) can use the X509 variable. Only this topic will bypass {ForceAuthentication}. Changing and renaming this topic should be restricted to the TwikiAdminGroup.

### {Plugins}{X509UserPlugin}{RequireWikinameFromCertificate}

Select this option to force a user's WikiName to be derived from his/her X.509 distingushed name. When not selected, the user's WikiName is suggested from the certificate name, but can be overridded by the registration form.

### {Plugins}{X509UserPlugin}{RegisterInUsersTopic}

Select this option if you want users registerd in the %UsersWeb.%UsersTopicName%. This is handy, but not required.

### {Plugins}{X509UserPlugin}{RegisterUsersWithLoginName}

X.509 certificate names not only look like line noise, they often contain characters that will confuse TWiki if they are placed on the Users Topic. By default, they are omitted. If you really want to deal with the problems, set this option.

### {Plugins}{X509UserPlugin}{Cert2Wiki}

Certificate authorities vary greatly in how they format a DN.

While the X509UserMapping code isn't infinitely flexible, it does allow the TWiki administrator to specify how to derive a wikiname from their certificates' DNs.

{X509UserPlugin}{Cert2Wiki} specifies the algorithm as a mapping string.

The mapping string is parsed into commands to fetch and format elements of the DN. The string is applied to the DN iteratively.

Each pass applies all the commands specified for that pass. If the resultingWikiname is unique, it stops. If not, it tries again, adding the commands for the next pass.

If the name still isn't unique after all commands have been tried, a sequence number is added to the result of the last pass.

Commands in the mapping string are separated by spaces.

Each command consists of optional flags, an element name, and an optional formatter.

The flags are:

- **^** will ucfirst each word in an element of the DN
- **n?** - will add this element in the nth pass only if the generated name is ambiguous at the start of the pass.

The **element name** is as found in the DN. If a name (such as OU) occurs more than once, the second occurance will be name.2; the third name.3 and so on.

The formatter is applied to the element as an s/// command. The formatter must contain its delimiters, and any flags. You can use this to extract or re-order subfields of an element, or pretty much anything else that's necessary.

After the formatter runs, any remaining spaces are removed (they're not valid in a wikiname).

A given element can be used as many or as few times as required. If an element isn't present in a particular certificate, its formatter will not be applied.

If the formatter is sufficiently ugly, you may need to quote the whole command.

Some examples:

The default of `^CN` will give `/CN=John a McSmith` the WikiName JohnAMcSmith.

`"^CN/(\w+), (.)/$2$1/" ^OU.2` would give `/OU=megalith/OU=widget sales/CN=smith, jan` the WikiName JanSmithWidgetSales.

If you want the first `smith, jan` to be JanSmith, but subsequent to be JanSmithWidgetSales, you might use `"CN{^(\w+),\s*(.*)$}($2$1)" ^1?OU.2/^([\w\s-]*?)(Department|Dept|Group|Team).*$/$1/`

There's quite a bit of room for creativity to mapthe often stilted formats used by the Certificate Authorities into friendly WikiNames. Or not - whatever meets your needs.

Quotes are necessary only if you embed spaces in your regexp. You can \-quote your quote - but any other \ is sent as-is to the s-command.

## Update your Registration topic

A sample is provided in the sandbox. You'll want to update it with your rules for filling out the fields from your certificates. The sample may work for you if your CN fields are Firstname {middle names, intitials...} Last name.

## Update your ResetPassword, ChangePassword, and ChangeEmail Topics

These don't apply to X.509 authentication - or when they do, they're some site-specific means of communicating with some other server. How to do that is beyond the scope of this document.

If you have a simple environment, you can simply make these topic say "No" (politely, of course.)

## Webserver configuration

Your webserver needs to be configured for SSL. Here is an extract of mine - an apache server. The key is how the `bin` directory is setup. You also need to setup the webserver's certificates - that's well documented elsewhere.

```
    DocumentRoot "/var/www/twiki/webroot"
    SSLOptions +FakeBasicAuth +StrictRequire +OptRenegotiate
    SSLVerifyClient require
    SSLVerifyDepth  10

    ScriptAlias /twiki/bin "/var/www/twiki/bin"
    Alias /twiki "/var/www/twiki"

    #Default / to /bin/view (which gets the main page)
    RedirectMatch ^/$ https://wiki.example.com/twiki/bin/view

<Directory "/var/www/twiki/bin">
    SSLOptions +StdEnvVars

    AllowOverride None
    Order Allow,Deny
    Allow from all
    Deny from env=blockAccess
    Satisfy all

    Options ExecCGI FollowSymLinks
    SetHandler cgi-script

    AuthUserFile /var/www/twiki/data/.htpasswd
    AuthName 'Select your personal identity certificate for wiki access, or click "cancel" to reg
    AuthType Basic

    # File to return on access control error (e.g. no certificate)
   ErrorDocument 401 /twiki/bin/view/Main/TWikiRegistration

    <FilesMatch "(passwd).*">
   Order Deny,Allow
   Deny from all
   # The images are inserted to ensure that the error page is above the
   # microsoft threshhold (512 bytes) for "friendly error messages".
   ErrorDocument 403 "<img src=\"/Images/topleftimage.gif\"> \
<B>This site is protected by X.509 certificates. Password resets are neither useful or permitted.
<img src=\"/Images/toprightimage.gif\">"
    </FilesMatch>

    <FilesMatch "^(configure)$">
   SetHandler cgi-script
   Order Deny,Allow
   Deny from all
   Allow from SpecificWorkstations.example.com

   AuthName 'example.com personal identity certificate must be authorized for wiki administrtion'
   Require user   "/C=..."
```

```
   ErrorDocument 401 default
   Satisfy all
    </FilesMatch>

    # When using Apache type login the following defines the TWiki scripts
    # that makes Apache ask the browser to authenticate. It is correct that
    # the view script is not authenticated, as it's used for registration.

    <FilesMatch "(attach|edit|manage|rename|save|upload|mail|logon|rest|.*auth).*">
   require valid-user
    </FilesMatch>
</Directory>
```

# Plugin Info

- Set SHORTDESCRIPTION = Authenticate & identify users using X.509 certificates

| | |
|---|---|
| Plugin Author: | TWiki:Main.TimotheLitt |
| Copyright: | © 2007, 2008, TWiki:Main.TimotheLitt |
| License: | GPL (GNU General Public License ) |
| Plugin Version: | 20 Oct 2008 (V1.0-1) |
| Change History: | |
| 26 Oct 2008: | V1.0-3 Correct documentation of configuration parameters |
| 24 Oct 2008: | V1.0-2 Return better status from X509UserMapping:removeUser |
| 20 Oct 2008: | Initial version |
| TWiki Dependency: | $TWiki::Plugins::VERSION 1.2, TWiki 4.2.3 |
| CPAN Dependencies: | none |
| Other Dependencies: | none |
| Perl Version: | 5.8.8 |
| Benchmarks : | GoodStyle nn%, FormattedSearch nn%, X509UserPlugin nn% |
| Plugin Home: | http://TWiki.org/cgi-bin/view/Plugins/X509UserPlugin |
| Feedback: | http://TWiki.org/cgi-bin/view/Plugins/X509UserPluginDev |
| Appraisal: | http://TWiki.org/cgi-bin/view/Plugins/X509UserPluginAppraisal |

***Related Topics:*** TWikiPlugins, DeveloperDocumentationCategory, AdminDocumentationCategory, TWikiPreferences

%TOPICCREATE{ template="Plugins.PluginDevTemplate" topic="X509UserPluginDev" disable="NewPluginTemplate" parameters="pluginName=X509UserPlugin&RelatedTopics=X509UserPlugin, X509UserPluginAppraisal" }% %TOPICCREATE{ template="Plugins.PluginAppraisalTemplate" topic="X509UserPluginAppraisal" disable="NewPluginTemplate" parameters="RelatedTopics=X509UserPlugin, X509UserPluginDev" }%

-- TWiki:Main.TimotheLitt - 20 Oct 2008

---

This topic: TWiki > X509UserPlugin
Topic revision: r3 - 2011-10-27 - TWikiAdminUser


***Note:*** Please contribute updates to this topic on TWiki.org at TWiki:TWiki.X509UserPlugin.